

## TRAITE D'COOPERATION EN MATIERE DE BREVETS

PCT

## NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Expéditeur: le BUREAU INTERNATIONAL

Destinataire:

Commissioner  
US Department of Commerce  
United States Patent and Trademark  
Office, PCT  
2011 South Clark Place Room  
CP2/5C24  
Arlington, VA 22202  
ETATS-UNIS D'AMERIQUE

en sa qualité d'office élu

<b>Date d'expédition (jour/mois/année)</b> 09 novembre 2000 (09.11.00)	<b>Référence du dossier du déposant ou du mandataire</b> GEM0701
<b>Demande internationale no</b> PCT/FR00/00283	<b>Date de priorité (jour/mois/année)</b> 08 mars 1999 (08.03.99)
<b>Date du dépôt international (jour/mois/année)</b> 07 février 2000 (07.02.00)	
<b>Déposant</b> BENOIT, Olivier	

1. L'office désigné est avisé de son élection qui a été faite:

☒ dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

23 septembre 2000 (23.09.00)

☐ dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection ☒ a été faite  
☐ n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

<b>Bureau international de l'OMPI</b> 34, chemin des Colombettes 1211 Genève 20, Suisse	<b>Fonctionnaire autorisé</b> Henrik Nyberg
no de télécopieur: (41-22) 740.14.35	no de téléphone: (41-22) 338.83.38

# TRAITE DE COOPERATION EN MATIERE DE BREVETS

## PCT

### RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire <b>GEM0701</b>	<b>POUR SUITE A DONNER</b> voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
Demande internationale n° <b>PCT/FR 00/ 00283</b>	Date du dépôt international (jour/mois/année) <b>07/02/2000</b>	(Date de priorité (la plus ancienne) (jour/mois/année) <b>08/03/1999</b>
Déposant <b>GEMPLUS et al.</b>		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 2 feuilles.

☒ Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

**1. Base du rapport**

a. En ce qui concerne la langue, la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

☐ la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

b. En ce qui concerne les séquences de nucléotides ou d'acides aminés divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

☐ contenu dans la demande internationale, sous forme écrite.

☐ déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

☐ remis ultérieurement à l'administration, sous forme écrite.

☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

☐ La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

☐ La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. ☐ Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche (voir le cadre I).

3. ☐ Il y a absence d'unité de l'invention (voir le cadre II).

**4. En ce qui concerne le titre,**

☒ le texte est approuvé tel qu'il a été remis par le déposant.

☐ Le texte a été établi par l'administration et a la teneur suivante:

**5. En ce qui concerne l'abrégé,**

☒ le texte est approuvé tel qu'il a été remis par le déposant

☐ le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure des dessins à publier avec l'abrégé est la Figure n°

☒ suggérée par le déposant.

☐ parce que le déposant n'a pas suggéré de figure.

☐ parce que cette figure caractérise mieux l'invention.

9

☐ Aucune des figures n'est à publier.

# RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No

PCT/FR 00/00283

**A. CLASSEMENT DE L'OBJET DE LA DEMANDE**  
CIB 7 H04L9/06

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

**B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE**

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

**C. DOCUMENTS CONSIDERES COMME PERTINENTS**

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	<p>NAKAO Y ET AL: "THE SECURITY OF AN RDES CRYPTOSYSTEM AGAINST LINEAR CRYPTANALYSIS" IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS, COMMUNICATIONS AND COMPUTER SCIENCES, JP, INSTITUTE OF ELECTRONICS INFORMATION AND COMM. ENG. TOKYO, vol. E79-A, no. 1, page 12-19 XP000558714 ISSN: 0916-8508 page 12, colonne de droite, ligne 8 -page 13, colonne de droite, ligne 23</p>	1

☐ Voir la suite du cadre C pour la fin de la liste des documents

☐ Les documents de familles de brevets sont indiqués en annexe

\* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

7 avril 2000

Date d'expédition du présent rapport de recherche internationale

17/04/2000

Nom et adresse postale de l'administration chargée de la recherche internationale

Office Européen des Brevets, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

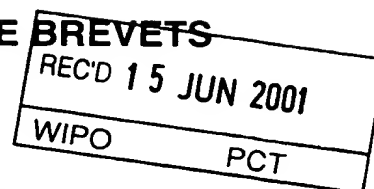
Fonctionnaire autorisé

Holper, G

09/1936202

## TRAITE DE COOPERATION EN MATIERE DE BREVETS

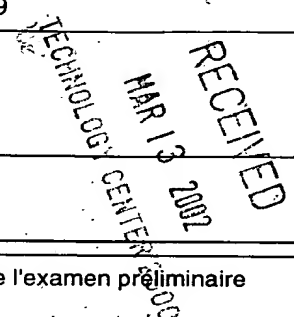
PCT



## RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire GEM 701	<b>POUR SUITE A DONNER</b> voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/FR00/00283	Date du dépôt international (jour/mois/année) 07/02/2000	Date de priorité (jour/mois/année) 08/03/1999
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L9/06		
Déposant GEMPLUS et al.		




1. Le présent rapport d'examen préliminaire international, établi par l'administration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.
2. Ce RAPPORT comprend 7 feuilles, y compris la présente feuille de couverture.
  - ☒ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

Ces annexes comprennent 19 feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

- I ☒ Base du rapport
- II ☐ Priorité
- III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
- IV ☐ Absence d'unité de l'invention
- V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
- VI ☒ Certains documents cités
- VII ☐ Irrégularités dans la demande internationale
- VIII ☒ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale 23/09/2000	Date d'achèvement du présent rapport 13.06.2001
Nom et adresse postale de l'administration chargée de l'examen préliminaire international:  Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé  Grimaldo, M  N° de téléphone +49 89 2399 7513



# RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR00/00283

## I. Base du rapport

1. En ce qui concerne les **éléments** de la demande internationale (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17)*):

### Description, pages:

1-6	version initiale			
7-22	reçue(s) le	12/03/2001	avec la lettre du	07/03/2001

### Revendications, N°:

1-8	reçue(s) le	12/03/2001	avec la lettre du	07/03/2001
-----	-------------	------------	-------------------	------------

### Dessins, feuilles:

1/8-8/8	version initiale
---------	------------------

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

- ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).
- ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).
- ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

- ☐ contenu dans la demande internationale, sous forme écrite.
- ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.
- ☐ remis ultérieurement à l'administration, sous forme écrite.
- ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
- ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
- ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listage des séquences Présenté par écrit, a été fournie.

**RAPPORT D'EXAMEN  
PRÉLIMINAIRE INTERNATIONAL**

Demande internationale n° PCT/FR00/00283

4. Les modifications ont entraîné l'annulation :

- ☐ de la description, pages :
- ☐ des revendications, n°s :
- ☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

*(Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)*

6. Observations complémentaires, le cas échéant :

**V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration**

1. Déclaration

Nouveauté	Oui : Revendications 1-8
	Non : Revendications
Activité inventive	Oui : Revendications 1-8
	Non : Revendications
Possibilité d'application industrielle	Oui : Revendications 1-8
	Non : Revendications

2. Citations et explications  
**voir feuille séparée**

**VI. Certain documents cités**

1. Certains documents publiés (règle 70.10)  
et / ou

2. Divulgations non écrites (règle 70.9)

**voir feuille séparée**

**VIII. Observations relatives à la demande internationale**

Les observations suivantes sont faites au sujet de la clarté des revendications, de la description et des dessins et de la question de savoir si les revendications se fondent entièrement sur la description :  
**voir feuille séparée**

**Documents mentionnés:**

Il est fait référence au document suivant:

D1: NAKAO Y ET AL: "THE SECURITY OF AN RDES CRYPTOSYSTEM AGAINST LINEAR CRYPTANALYSIS", IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS, COMMUNICATIONS AND COMPUTER SCIENCES, JP, INSTITUTE OF ELECTRONICS INFORMATION AND COMM. ENG. TOKYO, vol. E79-A, no. 1, page 12-19  
XP000558714 ISSN: 0916-8508

**V. Déclaration motivée selon la règle 66.2.a)ii) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration**

1. Les revendications indépendantes 1, 7 et 8 manquent de caractéristiques techniques essentielles (voir la section VIII, paragraphes 1a, 1b et 2).

Cependant, si les revendications 1, 7 et 8 sont interprétées à l'aide de la description qui spécifie les caractéristiques techniques essentielles manquantes, alors il est possible de comprendre que ces revendications concernent un procédé de contre-mesure pour protéger un algorithme DES à clé secrète d'une attaque DPA (Differential Power Analysis) (revendication 1), un composant électronique de sécurité mettant en oeuvre le procédé (revendication 7) et une carte à puce comprenant un tel composant électronique de sécurité (revendication 8).

Les algorithmes à clé secrète du type DES (Data Encryption standard) sont vulnérables aux attaques DPA consistant en une analyse différentielle de la consommation en courant, qui permettent à des tiers mal intentionnés de trouver la clé secrète.

Ces attaques sont destinées à découvrir la clé secrète en attaquant un nombre limité de bits particuliers de la clé: une sous-clé. A cette sous-clé correspondent certaines données en sortie de certaines opérations de l'algorithme de

cryptographie (opérations critiques: celles qui manipulent une donnée de sortie d'une opération SBOX) qui peuvent être plus facilement prédites: les bits de ces données sont appelés bits cibles.

Avec une attaque DPA qui analyse quand le signal DPA n'est pas nul en correspondance des instructions critiques on est capable de reconstituer la clé secrète, faisant un hypothèse sur la sous-clé.

Avec une attaque DPA sur un algorithme DES, composé de plusieurs tours de calcul, qui utilise une clé de 64 bits, on est capable de reconstituer au moins 48 bits des 56 bits utiles de la clé secrète.

La demande présente une solution à ce problème en utilisant un procédé dans un composant électronique de sécurité qui entraîne un signal DPA nul même dans le cas où l'hypothèse de sous clé est juste car, si le signal est nul, on n'obtient aucune information sur le bits cibles et donc sur la clé secrète. De cette façon rien ne permet de distinguer le cas de l'hypothèse de sous-clé juste des cas d'hypothèse de sous-clés fausses.

Le signal DPA nul, sur est obtenu par:

- a) l'application par chaque tour de calcul, qui compose le procédé, d'une opération de OU EXCLUSIF entre la donnée d'entrée et la donnée de sortie et une première valeur aléatoire (u).

En plus pour éviter des attaques qui pourraient être réalisées avec succès à des endroits bien déterminés dans l'exécution de l'algorithme, notamment en entrée et en sortie de l'ensemble des tours de calcul qui composent l'algorithme, le procédé applique:

- b) une opération de OU EXCLUSIF entre les données d'entrée du premier tour et une deuxième valeur aléatoire (v).

Le document D1, considéré comme représentant l'état de la technique le plus pertinent, divulgue également une modification d'un algorithme à clé secrète du type DES pour obtenir une meilleure protection contre une attaque DPA.

La modification comporte l'adjoint d'une opération d'échange (permutation) des données dans chaque tour de calcul de l'algorithme: le nouveau algorithme est appelé: RDES.

Cependant le document D1 ne divulgue pas les mêmes opérations décrites aux



points (a) et (b).

La solution n'est donc ni connue ni dérivable du document le plus proche (D1), et donc, l'objet de la revendication 1 est considéré comme nouveau (Article 33(2) PCT) et impliquant une activité inventive (Article 33(3) PCT).

2. Les revendications 2-6 dépendent de la revendication 1 et satisfont donc également, en tant que telles, aux conditions requises par le PCT en ce qui concerne la nouveauté et l'activité inventive.

#### **VI. Certains documents publiés (Règle 70.10)**

Demande n° Brevet n°	Date de publication (jour/mois/année)	Date de dépôt (jour/mois/année)	Date de priorité (valablement revendiquée) (jour/mois/année)
WO 00 27068	11/05/2000	29/10/1999	29/10/1998

Le document WO 00 27068 (document de priorité: FR 98 13605), du même Demandeur, divulgue exactement la même solution de contre-mesure contre des attaques par analyse différentielle du point (a).

Toutefois, le point (b) constitue la nouvelle caractéristique technique eu égard à ce document.

#### **VIII. Observations relatives à la demande internationale**

- 1a. Il ressort clairement de la description (page 9, lignes 4-9 et figures 3 et 8) que la caractéristique suivante est essentielle à la définition de l'invention de la revendication 1:

- la première valeur aléatoire appliquée en OU EXCLUSIF à la donnée d'entrée et à la donnée de sortie des moyens de calcul de chaque tour de calcul

La revendication indépendante 1 ne contenant pas cette caractéristique, ne remplit pas la condition visée à l'Article 6 PCT en combinaison avec la règle 6.3 b) PCT, qui prévoient qu'une revendication indépendante doit contenir toutes les caractéristiques techniques essentielles à la définition de l'invention.

1b. Il ressort clairement de la description (page 9, lignes 4-9, page 18, lignes 25-27 et figures 3 et 8) que la caractéristique suivante est essentielle à la définition de l'invention de la revendication 7:

- la première valeur aléatoire appliquée en OU EXCLUSIF à la donnée d'entrée et à la donnée de sortie des moyens de calcul de chaque tour de calcul
- la deuxième valeur aléatoire appliquée en OU EXCLUSIF AUX DONNÉES D'ENTRÉE de l'algorithme

La revendication indépendante 7 ne contenant pas cette caractéristique, ne remplit pas la condition visée à l'Article 6 PCT en combinaison avec la règle 6.3 b) PCT, qui prévoient qu'une revendication indépendante doit contenir toutes les caractéristiques techniques essentielles à la définition de l'invention.

2. Le jeu de revendications manque de clarté à cause du manque de cohérence entre la revendication de procédé 1 et la revendication d'appareil 7 (composant électronique): les caractéristiques techniques qui définissent l'objet de la protection recherchée ne sont pas les mêmes dans les deux revendications (Article 6 PCT).

## PATENT COOPERATION TREATY

## PCT

## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference GEM0701	<b>FOR FURTHER ACTION</b> See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/FR00/00283	International filing date (day/month/year) 07 February 2000 (07.02.00)	Priority date (day/month/year) 08 March 1999 (08.03.99)
International Patent Classification (IPC) or national classification and IPC H04L 9/06		
Applicant GEMPLUS		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of <u>7</u> sheets, including this cover sheet.  <input checked="" type="checkbox"/> This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).  These annexes consist of a total of <u>19</u> sheets.
3. This report contains indications relating to the following items:  I <input checked="" type="checkbox"/> Basis of the report II <input type="checkbox"/> Priority III <input type="checkbox"/> Non-establishment of opinion with regard to novelty, inventive step and industrial applicability IV <input type="checkbox"/> Lack of unity of invention V <input checked="" type="checkbox"/> Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement VI <input checked="" type="checkbox"/> Certain documents cited VII <input type="checkbox"/> Certain defects in the international application VIII <input checked="" type="checkbox"/> Certain observations on the international application

Date of submission of the demand 23 September 2000 (23.09.00)	Date of completion of this report 16 June 2001 (16.06.2001)
Name and mailing address of the IPEA/EP  Facsimile No.	Authorized officer  Telephone No.

## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR00/00283

## I. Basis of the report

## 1. With regard to the elements of the international application:\*

- ☐ the international application as originally filed
- ☒ the description:  
pages \_\_\_\_\_ 1-6 \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_ 7-22 \_\_\_\_\_, filed with the letter of \_\_\_\_\_ 12 March 2001 (12.03.2001)
- ☒ the claims:  
pages \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, as amended (together with any statement under Article 19  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_ 1-8 \_\_\_\_\_, filed with the letter of \_\_\_\_\_ 12 March 2001 (12.03.2001)
- ☒ the drawings:  
pages \_\_\_\_\_ 1/8-8/8 \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_
- ☐ the sequence listing part of the description:  
pages \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.  
These elements were available or furnished to this Authority in the following language \_\_\_\_\_ which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages \_\_\_\_\_
- ☐ the claims, Nos. \_\_\_\_\_
- ☐ the drawings, sheets/fig \_\_\_\_\_

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).\*\*

\* Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).

\*\* Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.

# INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.  
PCT/FR 00/00283

## V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

### 1. Statement

Novelty (N)	Claims	1-8	YES
	Claims		NO
Inventive step (IS)	Claims	1-8	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-8	YES
	Claims		NO

### 2. Citations and explanations

Reference is made to the following document:

D1: NAKAO Y ET AL: "THE SECURITY OF AN RDES CRYPTOSYSTEM AGAINST LINEAR CRYPTANALYSIS", IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS, COMMUNICATIONS AND COMPUTER SCIENCES, JP, INSTITUTE OF ELECTRONICS INFORMATION AND COMM. ENG. TOKYO, Vol. E79-A, no. 1, pages 12-19 XP000558714 ISSN: 0916-8508.

1. Independent Claims 1, 7 and 8 lack essential technical features (see Box VIII, paragraphs 1a, 1b and 2).

However, if Claims 1, 7 and 8 are interpreted in light of the description, which specifies the missing essential technical features, then it is clear that said claims relate to a countermeasure method for protecting a DES secret key algorithm from a DPA (Differential Power Analysis) attack (Claim 1), an electronic security component used with said method (Claim 7) and a smart card including such an electronic security component (Claim 8).

The DES (Data Encryption Standard) secret key algorithms are vulnerable to DPA attacks comprising a differential analysis of the current consumption that enable hackers to discover the secret key. These attacks are designed to discover the secret key by attacking a limited number of particular bits of the key, i.e. a sub-key. This sub-key represents certain output data from certain operations of the cryptography algorithm (critical operations are those that process output data from an SBOX operation) that can be easily predicted; the bits of said data are called target bits.

The secret key can be restored by hypothesizing on the sub-key, with a DPA attack that analyzes when the DPA is non-zero in correlation with the critical commands.

At least 48 of the 56 useful bits of the secret key can be restored with a DPA attack that uses a 64-bit key on a DES algorithm comprised of a number of calculation cycles.

The application provides a solution to this problem by using, in an electronic security component, a method that produces a zero DPA signal even when the hypothesis of the sub-key is correct, because if the signal is zero, information regarding the target bits, and thus the secret key, cannot be obtained. For this reason, there is nothing to distinguish between the case of the correct sub-key hypothesis and the incorrect sub-key hypothesis.

The zero DPA signal is obtained by:

(a) applying, for each calculation cycle of the method, an exclusive OR operation between the input data and the output data and a first random value

(u).

Moreover, to avoid attacks that could be successfully carried out at predetermined locations in the execution of the algorithm, particularly at the input and output of all the calculation cycles of the algorithm, the method applies:

(b) an exclusive OR operation between the input data of the first cycle and a second random value (v).

Document D1, which is considered the most relevant prior art, also discloses modifying a DES secret key algorithm in order to achieve better protection against a DPA attack.

The modification comprises adding an operation for exchanging (permutating) the data in each algorithm calculation cycle. The new algorithm is called RDES.

However, document D1 does not disclose the same operations as described in points (a) and (b).

The solution is therefore not found in or derivable from the closest prior art document (D1).

Consequently, the subject matter of Claim 1 is considered to be novel (PCT Article 33(2)) and to involve an inventive step (PCT Article 33(3)).

2. Claims 2-6 are dependent on Claim 1 and therefore also meet, as such, the PCT requirements of novelty and inventive step.

# INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR 00/00283

## Supplemental Box

(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: VI

Document WO-A-00/27068 (priority document: FR-A-9 813 605), by the same applicant, discloses exactly the same attack countermeasure solution as point (a) involving differential analysis.

However, point (b) is the novel technical feature in view of said document.



## VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

1a. It is clear from the description (page 9, lines 4-9 and Figures 3 and 8) that the following feature is essential to the definition of the invention of Claim 1:

- the first random value applied as exclusive OR to the input data and output data of the calculation means of each calculation cycle.

Since independent Claim 1 does not contain this feature, it does not meet the requirements of PCT Article 6 in combination with PCT Rule 6.3(b), according to which an independent claim must contain all the features necessary for the definition of the invention.

1b. It is clear from the description (page 9, lines 4-9, page 18, lines 25-27 and Figures 3 and 8) that the following features are essential to the definition of the invention of Claim 7:

- the first random value applied as exclusive OR to the input data and output data of the calculation means of each calculation cycle,
- the second random value applied as exclusive OR to the input data of the algorithm.

Since independent Claim 7 does not contain this feature, it does not meet the requirements of PCT Article 6 in combination with PCT Rule 6.3(b), according to which an independent claim must contain

# INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.  
PCT/FR 00/00283

## VIII. Certain observations on the international application

all the features necessary for the definition of the invention.

2. The set of claims lacks clarity owing to the inconsistency between method Claim 1 and device Claim 7 (electronic component). The technical features that define the subject matter for which protection is sought are not the same in the two claims (PCT Article 6).

figure 2). Il faut retourner à l'étape c- et faire une nouvelle hypothèse sur la sous-clé.

Si l'hypothèse s'avère juste, on peut passer à l'évaluation d'autres sous-clés, jusqu'à avoir reconstitué la clé au maximum. Par exemple, avec un  
5     algorithme DES, on utilise une clé de 64 bits, dont seulement 56 bits utiles. Avec une attaque DPA, on est capable de reconstituer au moins 48 bits des 56 bits utiles.

10     Deux documents concernant l'arrière plan technologique sont cités ci-dessous. Il s'agit des documents NAKAO Y ET AL : « THE SECURITY OF AN RDES CRYPTOSYSTEM AGAINST LINEAR CRYPTANALYSIS », IEICE  
15     TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS, COMMUNICATIONS AND COMPUTER SCIENCES, JP, INSTITUTE OF ELECTRONICS INFORMATION AND COMM.ENG.TOKYO , vol.E79-A, no.1, page 12-19 XP000558714 ISSN :0916-8508, noté D1 et WO 00 27068, noté D2.

20     Le document D1 concerne un cryptosystème utilisant le DES pour être sécurisé.

25     Le Document D2 concerne un composant électronique mettant en œuvre un algorithme à clé secrète ; la mise en œuvre de cet algorithme comprend l'utilisation de premiers moyens à partir d'une donnée d'entrée (E) pour fournir une donnée de sortie.

30     La présente invention a pour but de mettre en œuvre dans un composant électronique, un procédé de contre-mesure contre des attaques par analyse différentielle qui entraîne un signal DPA(t) nul, même dans le cas où l'hypothèse de sous-clé est juste.

35     De cette façon, rien ne permet de distinguer le cas de l'hypothèse de sous-clé juste des cas d'hypothèses de sous-clé fausses. Par cette contre-mesure, le composant électronique est paré contre les attaques DPA.

On sait par la demande française FR 2 785 477  
publiée le 5 Mai 2000, par la société GEMPLUS et dont  
le contenu en entier fait partie intégrante de la  
présente demande, qu'il ne suffit pas de faire en sorte  
5 que le signal  $DPA(t)$  soit nul relativement à un bit  
cible donné.

En effet, si on considère la valeur prise par  
plusieurs bits cibles d'une même donnée manipulée par  
les instructions critiques, on va devoir trier les  
10 courbes non plus en deux paquets, mais en plusieurs  
paquets. On n'a plus une fonction de sélection binaire.  
On peut montrer qu'en regroupant ensuite ces paquets  
d'une manière ou d'une autre, on peut obtenir un signal  
 $DPA(t)$  non nul dans le cas d'une hypothèse de sous-clé  
15 juste, alors qu'il aurait été nul si l'on avait trié  
selon une fonction de sélection binaire sur un seul bit  
cible.

Prenons par exemple deux bits cibles d'une même  
donnée. Ces deux bits cibles peuvent prendre les 2<sup>2</sup>  
20 valeurs suivantes : "00", "01", "10" et "11".

En appliquant la fonction de sélection aux  $N=1000$   
courbes de consommation en courant mesurées, on obtient  
quatre paquets de courbes. Si le tri est juste, un  
premier paquet de 250 courbes environ correspond à la  
25 valeur "00", un deuxième paquet de 250 courbes environ  
correspond à la valeur "01", un troisième paquet de  
250 courbes environ correspond à la valeur "10" et un  
quatrième paquet de 250 courbes environ correspond à la  
valeur "11".

30 Si on regroupe les premier et quatrième paquets  
dans un premier groupe et les deuxième et troisième  
paquets dans un deuxième groupe, on obtient deux  
groupes qui ne sont pas équivalents.

Dans le premier groupe, les deux bits ont autant de  
35 chances de valoir "00" que de valoir "11". La valeur

moyenne aux instants critiques de toutes les courbes de consommation de ce groupe peut s'écrire :

$$M1(t_{Ci}) = [\text{consommation}("00") + \text{consommation}("11")] / 2$$

5 Dans le deuxième groupe, les deux bits ont autant de chances de valoir "01" que de valoir "10". La valeur moyenne aux instants critiques de toutes les courbes de consommation de ce groupe peut s'écrire :

$$M2(t_{Ci}) = [\text{consommation}("01") + \text{consommation}("10")] / 2$$

10 Si on fait la différence entre ces deux moyennes, on obtient un signal DPA(t) non nul. En d'autres termes, les deux groupes dont on compare les consommations moyennes n'ont pas un contenu équivalent.

15 Dans la demande française précitée, on a cherché à empêcher l'obtention d'un quelconque signal significatif au sens de l'attaque DPA. Quel que soit le nombre de bits cibles pris, quelle que soit la combinaison de paquets effectuée pour faire la comparaison des consommations moyennes, le signal DPA(t) sera toujours nul. Pour cela il faut obtenir des  
20 paquets équivalents, quel que soit le nombre de bits cibles considérés.

La demande française précitée propose comme solution à ces différents problèmes techniques, l'utilisation d'une valeur aléatoire dans une opération  
25 de OU EXCLUSIF avec au moins des données de sortie de moyens de calcul utilisés dans l'algorithme.

Avec l'utilisation d'une telle valeur aléatoire, les données manipulées par les instructions critiques deviennent imprédictibles tout en ayant un résultat  
30 juste en sortie de l'algorithme.

Dans l'invention, on s'est cependant rendu compte que des attaques pourraient encore être réalisées avec succès à des endroits bien déterminés dans l'exécution de l'algorithme, notamment en entrée et en sortie de  
35 l'algorithme.

La présente invention a pour objet un procédé de contre-mesure dans lequel ces attaques sont également rendues impossibles. Selon l'invention, on utilise une deuxième valeur aléatoire, appliquée sur les paramètres d'entrée de l'algorithme de cryptographie, dans une opération de ou EXCLUSIF. Cette deuxième valeur aléatoire se propage dans tout l'algorithme, en sorte que les données qui n'étaient pas protégées par la première valeur aléatoire le sont par la deuxième.

Ainsi, selon l'invention, selon l'endroit où l'on se trouve dans l'algorithme, les données sont protégées soit par la première valeur-aléatoire, soit par la deuxième, soit par une combinaison de ces deux valeurs-aléatoires.

Telle que caractérisée, l'invention concerne donc un procédé de contre-mesure dans un composant électronique mettant en oeuvre un algorithme cryptographique à clé secrète, dont la mise en œuvre comprend plusieurs tours de calculs successifs pour fournir à partir de premières données d'entrée appliquées au premier tour, des données finales en sortie du dernier tour permettant l'élaboration d'un message chiffré, chaque tour de calcul utilisant des moyens de calcul pour fournir une donnée de sortie à partir d'une donnée d'entrée, lesdits moyens de calcul comprenant l'application d'une première valeur aléatoire (u) pour obtenir en sortie une donnée imprédictible, caractérisé en ce que le procédé comprend l'utilisation des moyens d'application d'une deuxième valeur aléatoire aux-dites premières données d'entrée, selon une opération ou EXCLUSIF.

D'autres caractéristiques et avantages de l'invention sont détaillés dans la description suivante faite à titre indicatif et nullement limitatif et en référence aux dessins annexés, dans lesquels :

- les figures 1 et 2 déjà décrites représentent le signal  $DPA(t)$  que l'on peut obtenir en fonction d'une hypothèse sur une sous-clé de la clé secrète  $K$ , selon une attaque DPA;

5       - les figures 3 et 4 sont des organigrammes détaillés des premiers et derniers tours de l'algorithme DES, selon l'état de la technique;

10       - la figure 5 est un schéma-bloc de l'opération SBOX utilisée dans l'algorithme DES tel que présenté sur les figures 3 et 4;

      - la figure 6. montre un exemple de table de constantes élémentaire à une entrée et une sortie utilisée dans l'opération SBOX représentée sur la figure 5;

15       - les figures 7 et 8 représentent respectivement un organigramme d'exécution du DES et un organigramme détaillé des premiers tours, correspondant à un exemple d'application du procédé de contre mesure selon l'état de la technique ;

20       - la figure 9 représente un organigramme d'exécution du DES selon l'invention; et

      - la figure 10 représente un schéma-bloc simplifié d'une carte à puce comportant un composant électronique dans lequel le procédé de contre-mesure selon l'invention est mis en oeuvre.

25       Pour la bonne compréhension de l'invention, on va d'abord décrire l'algorithme cryptographique à clé secrète DES normal, sans procédé de contre-mesure. Cet algorithme DES comporte 16 tours de calcul, notés T1 à T16, comme représenté sur les figures 3 et 4.

30       Le DES débute par une permutation initiale IP sur le message d'entrée M (figure 3). Le message d'entrée M est un mot  $f$  de 64 bits. Après permutation, on obtient un mot  $e$  de 64 bits, que l'on coupe en deux pour former les paramètres d'entrée L0 et R0 du premier tour (T1).  
35       L0 est un mot  $d$  de 32 bits contenant les 32 bits de

poids forts du mot e. R0 est un mot h de 32 bits contenant les 32 bits de poids faibles du mot e.

La clé secrète K, qui est un mot q de 64 bits subit elle-même une permutation et une compression pour  
5 fournir un mot r de 56 bits.

Le premier tour comprend une opération EXP PERM sur le paramètre R0, consistant en une expansion et une permutation, pour fournir en sortie un mot l de 48 bits.

10 Ce mot l est combiné à un paramètre K1, dans une opération de type OU EXCLUSIF notée XOR, pour fournir un mot b de 48 bits. Le paramètre K1 qui est un mot m de 48 bits est obtenu du mot r par un décalage d'une position (opération notée SHIFT sur les figures 3 et 4)  
15 suivi d'une permutation et d'une compression (opération notée COMP PERM).

Le mot b est appliqué à une opération notée SBOX, en sortie de laquelle on obtient un mot a de 32 bits. Cette opération particulière sera expliquée plus en  
20 détail en relation avec les figures 5 et 6.

Le mot a subit une permutation P PERM, donnant en sortie le mot c de 32 bits.

Ce mot c est combiné au paramètre d'entrée L0 du premier tour T1, dans une opération logique de type OU  
25 EXCLUSIF, notée XOR, qui fournit en sortie le mot g de 32 bits.

Le mot h (=R0) du premier tour fournit le paramètre d'entrée L1 du tour suivant (T2) et le mot g du premier tour fournit le paramètre d'entrée R1 du tour suivant.  
30 Le mot p du premier tour fournit l'entrée r du tour suivant.

Les autres tours T2 à T16 se déroulent de façon similaire, excepté en ce qui concerne l'opération de décalage SHIFT qui se fait sur une ou deux positions  
35 selon les tours considérés.



Chaque tour  $T_i$  reçoit ainsi en entrée les paramètres  $L_{i-1}$ ,  $R_{i-1}$  et  $r$  et fournit en sortie les paramètres  $L_i$  et  $R_i$  et  $r$  pour le tour suivant  $T_{i+1}$ .

5 En fin d'algorithme DES (figure 4), le message chiffré est calculé à partir des paramètres  $L_{16}$  et  $R_{16}$  fournis par le dernier tour  $T_{16}$ .

Ce calcul du message chiffré  $C$  comprend en pratique les opérations suivantes :

- 10 - formation d'un mot  $e'$  de 64 bits en inversant la position des mots  $L_{16}$  et  $R_{16}$ , puis en les concaténant;
- application de la permutation  $IP^{-1}$  inverse de celle de début de DES, pour obtenir le mot  $f'$  de 64 bits formant le message chiffré  $C$ .

15 L'opération SBOX est détaillée sur les figures 5 et 6. Elle comprend une table de constantes  $TC_0$  pour fournir une donnée de sortie  $a$  en fonction d'une donnée d'entrée  $b$ .

En pratique, cette table de constantes  $TC_0$  se présente sous la forme de huit tables de constantes élémentaires  $TC_{01}$  à  $TC_{08}$ , chacune recevant en entrée 20 seulement 6 bits du mot  $b$ , pour fournir en sortie seulement 4 bits du mot  $a$ .

Ainsi, la table de constante élémentaire  $TC_{01}$  représentée sur la figure 6 reçoit comme donnée 25 d'entrée, les bits  $b_1$  à  $b_6$  du mot  $b$  et fournit comme donnée de sortie les bits  $a_1$  à  $a_4$  du mot  $a$ .

En pratique ces huit tables de constantes élémentaires  $TC_{01}$  à  $TC_{08}$  sont mémorisées en mémoire programme du composant électronique.

30 Dans l'opération SBOX du premier tour  $T_1$ , un bit particulier de la donnée  $a$  de sortie de la table de constante  $TC_0$  dépend de seulement 6 bits de la donnée  $b$  appliquée en entrée, c'est à dire de seulement 6 bits de la clé secrète  $K$  et du message d'entrée ( $M$ ).

35 Dans l'opération SBOX du dernier tour  $T_{16}$ , un bit particulier de la donnée  $a$  de sortie de la table de

constante  $TC_0$  peut être recalculé à partir de seulement 6 bits de la clé secrète  $K$  et du message chiffré  $(C)$ .

Or si on reprend le principe de l'attaque DPA, si on choisit un ou des bits de la donnée de sortie a  
5 comme bits cibles, il suffit de faire une hypothèse sur 6 bits de la clé  $K$ , pour prédire la valeur du ou des bits cibles pour un message d'entrée  $(M)$  ou de sortie  $(C)$  donné. En d'autres termes, pour le DES, il suffit de faire une hypothèse sur une sous-clé de 6 bits.

10 Dans une attaque DPA sur un tel algorithme pour un ensemble de bits cibles donné issu d'une table de constantes élémentaire donnée, on a donc à discriminer une hypothèse de sous-clé juste parmi 64 possibles.

Ainsi, à partir des bits de sortie des huit tables  
15 de constantes élémentaires  $TC_{01}$  à  $TC_{08}$ , on peut découvrir jusqu'à  $8 \times 6 = 48$  bits de la clé secrète, en faisant des attaques DPA sur des bits cibles correspondants.

Dans le DES, on trouve donc des instructions  
20 critiques au sens des attaques DPA au début de l'algorithme et à la fin. Ces instructions sont détaillées dans la demande française FR 98 13605 à laquelle on pourra se reporter utilement.

Et il ressort que toutes les données manipulées par  
25 des instructions critiques sont une donnée de sortie ou des données dérivées d'une donnée de sortie d'une opération SBOX de début et de fin de DES.

Le procédé de contre-mesure décrit dans la demande française précitée appliqué à cet algorithme DES  
30 consiste à rendre imprédictible chacune des données manipulées par les instructions critiques. Ainsi, quel que soit le ou les bits cibles utilisés, le signal  $DPA(t)$  sera toujours nul. Ce procédé de contre-mesure est appliqué aux instructions critiques de début de DES  
35 et aux instructions critiques de fin de DES.

En prenant les opérations SBOX comme premiers  
moyens de calcul pour fournir une donnée de sortie  $S=a$   
à partir d'une donnée d'entrée  $E=b$ , le procédé de  
contre-mesure de la demande française précitée appliqué  
5 à l'algorithme DES consiste à utiliser d'autres moyens  
de calcul à la place des premiers, pour rendre  
imprédictible la donnée de sortie, en sorte que cette  
donnée de sortie et/ou des données dérivées manipulées  
par les instructions critiques soient toutes  
10 imprédictibles.

Ces autres moyens peuvent comprendre différents  
moyens. Ils sont calculés à partir des premiers moyens  
en appliquant un OU exclusif avec une valeur aléatoire  
 $u$  (ou une valeur aléatoire dérivée) sur l'une et/ou sur  
15 l'autre des données d'entrée et de sortie des premiers  
moyens.

L'utilisation de cette valeur aléatoire  $u$  est telle  
que le résultat en sortie de l'algorithme, c'est à  
dire, le message chiffré  $C$  reste juste.

20 Les figures 7 et 8 représentent un exemple  
d'application de ce procédé de contre-mesure, qui  
correspond à la figure 10 de la demande française  
précitée.

Dans une exécution classique de l'algorithme DES,  
25 on a vu que chaque tour comprend l'utilisation de  
premiers moyens  $TC_0$  dans une opération SBOX.

Dans cet exemple, et comme représenté sur la figure  
7, on calcule d'autres moyens en faisant un OU EXCLUSIF  
avec une valeur aléatoire  $u$  sur les données de sortie  
des premiers moyens  $TC_0$  et en faisant un OU EXCLUSIF  
30 avec une valeur dérivée  $e(p(u))$  sur les données  
d'entrée des premiers moyens  $TC_0$ . Puis on applique une  
séquence SEQA d'exécution identique sur chaque groupe,  
qui consiste à utiliser ces autres moyens calculés.

35 Dans ce procédé, on utilise donc une valeur  
aléatoire  $u$  qui est une donnée de 32 bits. On peut par

exemple tirer une valeur aléatoire de 32 bits, ou bien tirer une valeur aléatoire de 4 bits et les recopier 8 fois pour obtenir la valeur aléatoire sur 32 bits.

On calcule alors la variable dérivée égale à  $e(p(u))$ , où  $p(u)$  correspond au résultat de l'opération P PERM appliquée sur la valeur  $u$  et où  $e(p(u))$  est le résultat de l'opération EXP PERM appliquée à la valeur  $p(u)$ .

On peut alors calculer les autres moyens utilisés par ce procédé de contre-mesure.

Dans l'exemple représenté en référence à la figure 7, ces autres moyens comprennent des deuxièmes moyens  $TC_2$  et une opération ou EXCLUSIF supplémentaire notée CP.

Les deuxièmes moyens  $TC_2$  sont utilisés dans chacun des tours.

Ils sont calculés en appliquant un OU EXCLUSIF avec la variable aléatoire dérivée  $e(p(u))$  sur la donnée d'entrée  $E$  et en appliquant un OU EXCLUSIF avec la valeur aléatoire  $u$  sur la donnée de sortie  $S$  des premiers moyens  $TC_0$ , ce qui peut s'écrire :  $TC_2 = (E \oplus e(p(u)), S \oplus u)$ .

L'opération OU EXCLUSIF supplémentaire CP avec la variable aléatoire dérivée  $e(p(u))$ , permet d'obtenir en entrée des deuxièmes moyens  $TC_2$  la donnée  $b \oplus e(p(u))$ . Cette opération est notée  $CP(e(p(u)))$  sur les figures 7 et 8.

Cette opération OU EXCLUSIF supplémentaire CP avec la variable  $e(p(u))$  peut être placée en divers endroits des premiers et derniers tours, soit entre l'opération EXP PERM et l'opération XOR ou entre l'opération XOR et l'opération SBOX. On peut la remplacer par une opération OU EXCLUSIF supplémentaire CP avec la variable aléatoire dérivée  $p(u)$ , en plaçant cette opération supplémentaire  $CP(p(u))$  avant l'opération EXP

PERM. On obtient en sortie  $l \oplus e(p(u))$ , et donc on aura ensuite  $b \oplus e(p(u))$ .

Dans tous ces cas de figures, on obtient la donnée  $b \oplus e(p(u))$  en entrée de l'opération SBOX.

5 Le programme de calcul consiste alors au début de l'exécution de l'algorithme, à tirer une valeur aléatoire  $u$ , dans l'exemple sur 4 bits, à calculer la variable aléatoire dérivée  $e(p(u))$ , puis à calculer les différents moyens utilisés dans la séquence d'exécution  
10 SEQA, c'est à dire calculer les deuxièmes moyens  $TC_2$ .

On obtient, à la sortie de chaque groupe, le résultat juste pour les paramètres de sortie. Ainsi, les paramètres de sortie  $L_4$  et  $R_4$  du premier groupe  $G_1$ ,  $L_8$  et  $R_8$  du deuxième groupe  $G_2$ ,  $L_{12}$  et  $R_{12}$  du troisième  
15 groupe  $G_3$ ,  $L_{16}$  et  $R_{16}$  du quatrième groupe  $G_4$  sont justes quelle que soit la variable aléatoire tirée.

Quand on a effectué tous les tours, on obtient les paramètres justes  $L_{16}$  et  $R_{16}$  qui vont permettre de calculer le message chiffré  $C$  juste.

20 Par contre, à l'intérieur des groupes, certains résultats intermédiaires n'ont pas les mêmes valeurs selon la séquence utilisée, mais des valeurs correspondant à l'opération OU EXCLUSIF avec la valeur aléatoire  $u$  ou avec la valeur aléatoire dérivée  
25  $e(p(u))$ , ce qui permet d'obtenir la protection contre les attaques DPA.

La figure 8 montre l'organigramme détaillé des quatre tours  $T_1$ ,  $T_2$ ,  $T_3$  et  $T_4$  du premier groupe  $G_1$ , dans la séquence SEQA, qui permet de mettre en évidence  
30 le rôle des deuxièmes moyens  $TC_2$  utilisés dans chaque tour. D'après leur définition :  $TC_2 = E \oplus e(p(u))$ ,  $S \oplus u$ , en appliquant en entrée la donnée modifiée aléatoirement  $b \oplus e(p(u))$  grâce à l'opération supplémentaire CP, on obtient en sortie la donnée  
35 modifiée aléatoirement  $a \oplus u$ . En conduisant ce raisonnement depuis le tour  $T_1$  jusqu'à la fin du tour

T4, et en remarquant que  $p(u) \oplus p(u) = 0$ , on obtient en sortie du tour T4, les données L4, R4 non modifiées.

5 Avec un tel procédé de contre-mesure, on doit prévoir en début de DES le tirage de la valeur aléatoire  $u$  et le calcul des moyens utilisés dans la séquence d'exécution SEQA. Ces moyens calculés à chaque  
exécution du DES, sont mémorisés, le temps de l'exécution, en mémoire de travail, les premiers moyens  $TC_0$  qui servent au calcul étant eux mémorisés en  
10 mémoire programme.

Ce procédé de contre-mesure selon l'état de la technique qui consiste donc de manière générale à appliquer une valeur aléatoire  $u$  au moins sur la sortie des moyens de calcul utilisés dans chaque tour de  
15 l'algorithme, laisse certaines données en clair. Sur les figures 7 et 8 on voit que les données d'entrée,  $L_0$ ,  $R_0$ , et à leur suite les données  $h$ ,  $l$  et  $b$  du premier tour sont utilisées en clair.

De même les données  $R_3$ ,  $L_4$ ,  $R_4$ ,  $R_7$ ,  $L_8$ ,  $R_8$ ,  $R_{11}$ ,  $L_{12}$ ,  $R_{12}$ ,  $R_{15}$ ,  $L_{16}$  et  $R_{16}$  sont utilisées en clair.  
20

D'une manière générale, quelque soit le mode d'application du procédé de contre-mesure de l'état de la technique qui vient d'être décrit, au moins les données d'entrée  $L_0$  et  $R_0$  et de sortie  $L_{16}$  et  $R_{16}$  sont  
25 utilisées en clair dans l'algorithme. D'autres données intermédiaires peuvent l'être, comme dans le cas précédemment décrit, qui dépendent plus particulièrement du mode d'application considéré du procédé de contre-mesure de l'état de la technique,  
30 dont les figures 7 et 8 ne montrent qu'un des exemples d'application.

En pratique, des attaques peuvent donc être encore réalisées sur l'algorithme, basées sur ces données utilisées en clair.

35 La présente invention propose donc un perfectionnement au procédé de contre-mesure précité,

qui permet de rendre imprédictibles toutes les données utilisées dans l'algorithme, soit par la première valeur aléatoire  $u$ , soit par une deuxième valeur aléatoire notée  $v$ , soit par une combinaison des deux.

5 Un exemple de mise en oeuvre de ce procédé est représenté sur la figure 9.

Selon l'invention, une deuxième valeur aléatoire notée  $v$  est utilisée, appliquée aux données d'entrée  $L0$  et  $R0$ , au moyen d'une opération OU EXCLUSIF.

10 Ainsi, les données d'entrée réellement utilisées dans le calcul de l'algorithme, sont des données imprédictibles égales à  $L0 \oplus v$  et  $R0 \oplus v$ .

Cette deuxième valeur aléatoire se propage dans chacun des tours de l'algorithme. En sortie du seizième tour  $T16$ , on obtient donc comme données de sortie, les données imprédictibles égales à  $L16 \oplus v$  et  $R16 \oplus v$ .

15 Pour retrouver les données de sortie vraies  $L16$  et  $R16$  qui vont permettre d'obtenir le message chiffré  $C$ , on applique sur chacune de ces données  $L16 \oplus v$  et  $R16 \oplus v$ , une opération OU EXCLUSIF avec la deuxième valeur aléatoire  $v$ .

L'utilisation des deux valeurs aléatoires  $u$  et  $v$  en combinaison permet d'obtenir un procédé de contre-mesure perfectionné, rendant inattaquable l'algorithme DES qui le met en oeuvre.

25 Sur la figure 9, on a détaillé un exemple de mise en oeuvre pratique d'un procédé de contre-mesure selon l'invention.

Si on prend le premier tour  $T1$ , on a en entrée les données  $L0 \oplus v$  et  $R0 \oplus v$  auxquelles on applique successivement les opérations EXP PERM, XOR (avec la clé  $K1$ ). On se retrouve donc en entrée de l'opération SBOX avec la donnée  $b \oplus v$ .

35 Les moyens de calcul  $TC_M$  associés à cette opération SBOX consistent comme dans le procédé de contre-mesure de l'état de la technique en une table de constantes

déduite de la table de constantes d'origine  $TC_0$  de l'algorithme DES.

En notant cette table de constantes d'origine  $TC_0 = (E, S)$  comme vu en relation avec la figure 6, on calcule les nouveaux moyens de calcul  $TC_M$  de la manière suivante :

$$TC_M = (E \oplus e(v), S \oplus u).$$

De cette manière, on tient compte de la deuxième valeur aléatoire  $v$  appliquée aux données en entrée de chaque tour, et on bénéficie toujours de la première valeur aléatoire,  $u$  selon le procédé de l'état de la technique, en sortie de l'opération SBOX.

Ainsi, en sortie de l'opération SBOX utilisant les moyens de calcul  $TC_M$ , on obtient la donnée  $a \oplus p(u)$ , sur laquelle on applique l'opération  $P$  PERM, donnant la donnée  $c \oplus p(u)$ .

L'opération XOR suivante avec la donnée d'entrée  $L0 \oplus v$  fournit en sortie la donnée  $g \oplus p(u) \oplus v$ .

On rappelle que dans l'état de la technique décrit (FIG.8), on obtenait à ce stade la donnée  $g \oplus p(u)$  utilisée en entrée du deuxième tour  $T2$ .

Avec le procédé selon l'invention, l'autre entrée du deuxième tour est la donnée  $L1 \oplus v = R0 \oplus v$ , comme indiqué sur la figure 9.

La deuxième valeur aléatoire  $v$  se propage donc dans tous les tours de l'algorithme.

Si on ne fait pas disparaître la valeur aléatoire  $u$  de la donnée de sortie du premier tour ( $R1 \oplus (v) \oplus p(u)$ ), il faut prévoir l'utilisation d'autres moyens de calcul  $TC_M'$  dans le deuxième tour  $T2$ , définis par  $TC_M' = E \oplus e(v) \oplus e(p(u)), S \oplus u$ .

Cette mise en oeuvre de l'invention n'est pas très intéressante, car elle nécessite le calcul de deux nouvelles tables de constantes  $TC_M$  et  $TC_M'$ , la valeur aléatoire  $u$  étant appliquée dans la table  $TC_M'$ , non seulement sur la sortie, mais aussi sur l'entrée.



Aussi, selon l'invention, et comme représenté sur la figure 9, pour faciliter l'utilisation des deux variables aléatoires  $u$  et  $v$  en réduisant les calculs nécessaires à sa mise en oeuvre et pour reproduire les mêmes opérations dans chaque tour, on prévoit une opération OU EXCLUSIF supplémentaire notée  $CP(p(u))$  en fin de chaque tour, de manière à faire disparaître la valeur  $p(u)$  en entrée de chaque nouveau tour. Ainsi, en entrée du deuxième tour  $T1$ , on obtient la donnée  $R1 \oplus v = (g \oplus p(u) \oplus v) \oplus p(u)$ , soit

$$R1 \oplus v = g \oplus v.$$

Chaque tour se succède alors en exécutant la même suite d'opérations de calcul, alors en sorte qu'en sortie du seizième tour, on obtient comme données de sortie,  $L16 \oplus v$  et  $R16 \oplus v$ . En appliquant une opération de OU EXCLUSIF avec la deuxième valeur aléatoire  $v$  sur chacune de ces deux données, on obtient les données  $L16$  et  $R16$  qui permettent l'élaboration du message chiffré  $C$ .

En appliquant le procédé de contre-mesure selon l'invention qui combine l'utilisation d'une première valeur aléatoire  $u$  dans des moyens de calculs prévus dans chaque tour et l'utilisation d'une deuxième valeur aléatoire appliquée en entrée, avant l'exécution du premier tour, on rend imprédictibles toutes les données utilisées dans l'algorithme. Selon l'endroit où l'on se trouve dans l'algorithme, la protection par contre-mesure selon l'invention est assurée soit par la première valeur aléatoire  $u$ , soit par la deuxième valeur aléatoire  $v$ , soit par une combinaison de ces deux valeurs.

En pratique, et dans l'exemple d'application représenté sur la figure 9, avant d'exécuter l'algorithme DES proprement dit, il faut exécuter les opérations suivantes :

- tirage des valeurs aléatoires  $u$  et  $v$

- calcul de  $p(u)$  pour l'opération  $CP(p(u))$
- calcul de  $e(v)$
- calcul de  $TC_M = E \oplus e(v), S \oplus u$ .

5 La valeur aléatoire  $v$  est une donnée comportant le même nombre bits que les données  $L0$  et  $R0$ , soit 32 bits dans l'exemple. Dans ce procédé, on utilise donc une valeur aléatoire  $v$  qui est une donnée de 32 bits. On peut par exemple tirer une valeur aléatoire de 32 bits, ou bien  
10 tirer une valeur aléatoire de 4 bits et les recopier 8 fois pour obtenir la valeur aléatoire sur 32 bits (comme pour la valeur aléatoire  $u$ ).

D'autres exemples d'application peuvent être envisagés, dans lesquels on peut notamment prévoir que les tours ne sont pas identiques. Toutes ces variantes  
15 qui utilisent les deux valeurs aléatoires selon le principe général exposé sont du domaine de l'invention.

Un composant électronique 1 mettant en oeuvre un procédé de contre-mesure selon l'invention dans un algorithme de cryptographie à clé secrète DES, comprend  
20 typiquement, comme représenté sur la figure 10, un microprocesseur  $mP$ , une mémoire programme 2 et une mémoire de travail 3. Les différents moyens de calcul  $TC_0$  et  $TC_M$  sont, en pratique, des tables de constantes mémorisées respectivement en mémoire programme 1 et en  
25 mémoire de travail 3. Pour pouvoir gérer l'utilisation, de ces moyens de calcul, des moyens 4 de génération d'une valeur aléatoire sont prévus qui, si on se reporte aux organigrammes des figures 7 et 11, fourniront les valeurs aléatoires  $u$  et  $v$  à chaque  
30 exécution du DES. Un tel composant peut tout particulièrement être utilisé dans une carte à puce 5, pour améliorer son inviolabilité.

## REVENDICATIONS

1. Procédé de contre-mesure contre des attaques par analyse différentielle dans un composant électronique mettant en oeuvre un algorithme cryptographique à clé secrète (K), dont la mise en oeuvre comprend plusieurs  
5 tours de calculs successifs (T1,...T16) pour fournir à partir de premières données d'entrée (L0, R0) appliquées au premier tour (T1), des données finales (L16, R16) en sortie du dernier tour (T16) permettant l'élaboration d'un message chiffré (C), chaque tour de  
10 calcul utilisant des moyens de calcul (TC) pour fournir une donnée de sortie (S) à partir d'une donnée d'entrée (E), lesdits moyens de calcul comprenant l'application d'une première valeur aléatoire (u) à la donnée d'entrée (E) et à la donnée de sortie (S) pour obtenir  
15 en sortie une donnée imprédictible ( $S \oplus u$ ), caractérisé en ce que le procédé comprend l'utilisation de moyens d'application d'une deuxième valeur aléatoire (v) aux-dites premières données d'entrée (L0, R0), selon une opération ou EXCLUSIF.

20 2. Procédé de contre-mesure selon la revendication 1, caractérisé en ce qu'il comprend en outre l'utilisation de moyens d'application de la deuxième valeur aléatoire (v) sur les données finales fournies  
25 par le dernier tour (T16), selon une opération ou EXCLUSIF.

3. Procédé de contre mesure selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend à la fin de chaque tour, l'exécution d'une opération supplémentaire ( $CP(p(u))$ ) pour faire

disparaître ladite première valeur aléatoire (u) en sortie de chaque tour.

5 4. Procédé de contre-mesure selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend le tirage des première et deuxième valeurs aléatoires (u, v) et le calcul des moyens de calcul ( $TC_M$ ) utilisés dans chaque tour pour chaque nouvelle exécution de l'algorithme.

10 5. Procédé selon la revendication 4, caractérisé en ce que les dits moyens de calculs ( $TC_M$ ) sont calculés à partir de premiers moyens de calculs ( $TC_0$ ) définissant pour des données d'entrée (E), des données de sortie (S) correspondantes, en appliquant la deuxième valeur aléatoire (v) aux dites données d'entrée ( $E \oplus v$ ) et en  
15 appliquant la première valeur aléatoire (u) au moins aux dites données de sortie ( $s \oplus u$ ) des premiers moyens de calcul.

20 6. Procédé de contre-mesure selon la revendication 5, caractérisé en ce que les moyens de calculs ( $TC_0$ ,  $TC_M$ ) sont des tables de constantes.

25 7. Composant électronique de sécurité mettant en oeuvre le procédé de contre-mesure contre des attaques par analyse différentielle comprenant un algorithme cryptographique à clé secrète (K), dont la mise en oeuvre comprend plusieurs tours de calculs successifs ( $T_1, \dots, T_{16}$ ) pour fournir à partir de premières données d'entrée ( $L_0$ ,  $R_0$ ) appliquées au premier tour ( $T_1$ ), des données finales ( $L_{16}$ ,  $R_{16}$ ) en sortie du dernier tour ( $T_{16}$ ) permettant l'élaboration d'un message chiffré  
30 (C), chaque tour de calcul utilisant des moyens de calcul (TC) pour fournir une donnée de sortie (S) à

partir d'une donnée d'entrée (E), lesdits moyens de calcul comprenant l'application d'une première valeur aléatoire (u) à la donnée d'entrée (E) et à la donnée de sortie (S) pour obtenir en sortie une donnée imprédictible ( $S \oplus u$ ), caractérisé en ce que des premiers moyens de calcul ( $TC_0$ ) sont fixés en mémoire programme (1) du dit composant, des moyens de calcul ( $TC_M$ ) utilisés dans chaque tour étant calculés à chaque nouvelle exécution de l'algorithme et mémorisés en mémoire de travail (3) et en ce qu'il comprend des moyens (4) de génération de premières et deuxièmes valeurs aléatoires (u, v) pour calculer les dits moyens de calcul ( $TC_M$ )

8. Carte à puce comprenant un composant électronique de sécurité selon la revendication 7.

d - predicting, for each of the random messages, the value taken by one of the target bits, the value of which depends only on the bits of the message (input or output) and the sub-key taken as a hypothesis, in order to obtain the Boolean selection function;

e - sorting the curves according to this Boolean selection function (that is to say according to the value "0" or "1" predicted for this target bit for each curve under the sub-key hypothesis);

f - calculating, in each bundle, the resultant mean current consumption curve;

g - calculating the difference of these mean curves, in order to obtain the signal  $DPA(t)$ .

If the hypothesis on the sub-key is correct, the Boolean selection function is correct and the curves in the first bundle actually correspond to the curves for which the message applied at the input or output gave a target bit at "0" in the card and the curves in the second bundle actually correspond to the curves for which the message applied at the input or output gave a target bit at "1" in the card.

This is the situation of Figure 1: the signal  $DPA(t)$  is therefore not null at the instants  $tc_0$  to  $tc_6$  corresponding to execution of the critical instructions (those which manipulate the target bit).

It should be noted that the attacker has no need to know the critical instants accurately. It is sufficient for there to be at least one critical instant in the acquisition period.

If the sub-key hypothesis is not correct, the sort does not correspond to reality and there are then in each bundle as many curves corresponding in reality to a target bit at "0" as curves corresponding to a target bit at "1". The signal  $DPA(t)$  is substantially null everywhere (the case depicted in Figure 2). It is necessary to return to step c - and make a new hypothesis on the sub-key.

If the hypothesis proves to be correct, the procedure can move to the evaluation of other sub-keys, until the key has been reconstructed as much as possible. For example, with a DES algorithm, use is made of a key of 64 bits, only 56 of which are useful. With a DPA attack, it is possible to reconstruct at least 48 bits of the 56 useful bits.

The aim of the present invention is to implement, in an electronic component, a countermeasure method which brings about a null signal  $DPA(t)$ , even where the sub-key hypothesis is correct.

In this way, nothing allows the correct sub-key hypothesis case to be distinguished from the false sub-key hypothesis cases. By means of this countermeasure, the electronic component is guarded against DPA attacks.

It is known through the French patent application FR 98 13605 filed on 29 October 1998 by the GEMPLUS company that it is not sufficient to arrange that the signal  $DPA(t)$  is null in relation to a given target bit.

This is because, if the value taken by a number of target bits of the same data item manipulated by the critical instructions is considered, the curves will have to be sorted, no longer into two bundles, but into a number of bundles. It is no longer a binary selection function. It can be shown that, by next grouping together these bundles in one way or another, a signal  $DPA(t)$  can be obtained which is non-null in the case of a correct sub-key hypothesis, whereas it would have been null if a sort had been performed according to a binary selection function on a single target bit.

Let, for example, two target bits of the same data item be taken. These two target bits can take the following  $2^2$  values: "00", "01", "10" and "11".

By applying the selection function to the  $N=1000$  measured current consumption curves, four bundles of curves are obtained. If the sort is correct, a first bundle of around 250 curves corresponds to the value "00", a second bundle of around 250 curves corresponds to the value "01", a third bundle of around 250 curves corresponds to the value "10" and a fourth bundle of around 250 curves corresponds to the value "11".

If the first and fourth bundles are grouped together in a first group and the second and third bundles are grouped together in a second group, two groups which are not equivalent are obtained.

In the first group, the two bits have as many chances of having the value "00" as having the value



"11". The mean value at the critical instants of all the consumption curves in this group can be written:

$$M1(t_{ci}) = [\text{consumption}("00") + \text{consumption}("11")]/2$$

In the second group, the two bits have as many chances of having the value "01" as having the value "10". The mean value at the critical instants of all the consumption curves in this group can be written:

$$M2(t_{ci}) = [\text{consumption}("01") + \text{consumption}("10")]/2$$

If the difference between these two means is calculated, a non-null signal  $DPA(t)$  is obtained. In other words, the two groups whose mean consumptions are being compared do not have an equivalent content.

In the aforementioned French patent application, an attempt has been made to prevent any significant signal in the DPA attack sense being obtained. Whatever the number of target bits taken, whatever the combination of bundles made for comparing the mean consumptions, the signal  $DPA(t)$  will always be null. For this, it is necessary to obtain equivalent bundles, whatever the number of target bits considered.

The aforementioned French patent application, as a solution to these various technical problems, proposes the use of a random value in an EXCLUSIVE OR operation with at least some output data from calculation means used in the algorithm.

With the use of such a random value, the data manipulated by the critical instructions become unpredictable while having a correct result at the output of the algorithm.

In the invention, however, it was ascertained that attacks could still be carried out successfully at well-determined locations in the algorithm execution, notably at the input and output of the algorithm.

The object of the present invention is a countermeasure method in which these attacks are also made impossible. According to the invention, a second random value is used, applied to the input parameters of the cryptographic algorithm, in an EXCLUSIVE OR operation. This second random value propagates through the whole algorithm, so that the data which were not protected by the first random value are protected by the second.

Thus, according to the invention, depending on the location in the algorithm, the data are protected either by the first random value, or by the second, or by a combination of these two random values.

As characterised, the invention therefore relates to a countermeasure method in an electronic component implementing a secret key cryptographic algorithm, the implementation of which comprises a number of successive calculation cycles in order to supply, from first input data applied to the first cycle, final data at the output of the last cycle allowing the production of an encrypted message, each calculation cycle using calculation means for supplying an output data item

from an input data item, said calculation means comprising the application of a first random value (u) in order to obtain at the output an unpredictable data item, characterised in that the method comprises the use of means of applying a second random value to said first input data, according to an EXCLUSIVE OR operation.

Other characteristics and advantages of the invention are detailed in the following description given as a guide and being in no way limitative and with reference to the accompanying drawings, in which:

- Figures 1 and 2, already described, depict the signal  $DPA(t)$  which can be obtained in accordance with a hypothesis on a sub-key of the secret key K, according to a DPA attack;

- Figures 3 and 4 are detailed flow diagrams of the first and last cycles of the DES algorithm, according to the state of the art;

- Figure 5 is a block diagram of the operation SBOX used in the DES algorithm as presented in Figures 3 and 4;

- Figure 6 shows an example elementary constants table with one input and one output used in the operation SBOX depicted in Figure 5;

- Figures 7 and 8 depict respectively an execution flow diagram of the DES and a detailed flow diagram of the first cycles, corresponding to an example application of the countermeasure method according to the state of the art;

- Figure 9 depicts an execution flow diagram of the DES according to the invention; and

- Figure 10 depicts a simplified block diagram of a smart card having an electronic component in which the countermeasure method according to the invention is implemented.

For a good understanding of the invention, the normal DES secret key cryptographic algorithm, with no countermeasure method, will first be described. This DES algorithm has 16 calculation cycles, denoted T1 to T16, as depicted in Figures 3 and 4.

The DES starts with an initial permutation IP on the input message M (Figure 3). The input message M is a 64-bit word f. After permutation, a 64-bit word e is obtained, which is cut into two in order to form the input parameters L0 and R0 of the first cycle (T1). L0 is a 32-bit word d containing the most significant 32 bits of the word e. R0 is a 32-bit word h containing the least significant 32 bits of the word e.

The secret key K, which is a 64-bit word q, itself undergoes a permutation and a compression in order to supply a 56-bit word r.

The first cycle comprises an operation EXP PERM on the parameter R0, consisting of an expansion and a permutation, in order to supply at the output a 48-bit word l.

This word l is combined with a parameter K1, in an EXCLUSIVE OR type operation denoted XOR, in order to supply a 48-bit word b. The parameter K1, which is a 48-bit word m, is obtained from the word r by a shift

of one position (the operation denoted SHIFT in Figures 3 and 4) followed by a permutation and a compression (the operation denoted COMP PERM).

The word  $b$  is applied to an operation denoted SBOX, at the output of which a 32-bit word  $a$  is obtained. This particular operation will be explained in more detail in connection with Figures 5 and 6.

The word  $a$  undergoes a permutation P PERM, giving at the output the 32-bit word  $c$ .

This word  $c$  is combined with the input parameter  $L_0$  of the first cycle  $T_1$ , in an EXCLUSIVE OR type logical operation, denoted XOR, which supplies at the output the 32-bit word  $g$ .

The word  $h$  ( $= R_0$ ) of the first cycle supplies the input parameter  $L_1$  of the next cycle ( $T_2$ ) and the word  $g$  of the first cycle supplies the input parameter  $R_1$  of the next cycle. The word  $p$  of the first cycle supplies the input  $r$  of the next cycle.

The other cycles  $T_2$  to  $T_{16}$  progress in a similar manner, except as regards the shift operation SHIFT which is carried out over one or two positions depending on the cycles considered.

Each cycle  $T_i$  thus receives at the input the parameters  $L_{i-1}$ ,  $R_{i-1}$  and  $r$  and supplies at the output the parameters  $L_i$  and  $R_i$  and  $r$  for the next cycle  $T_{i+1}$ .

At the end of the DES algorithm (Figure 4), the encrypted message is calculated from the parameters  $L_{16}$  and  $R_{16}$  supplied by the last cycle  $T_{16}$ .

This calculation of the encrypted message  $C$  in practice comprises the following operations:

- formation of a 64-bit word  $e'$  by reversing the position of the words  $L16$  and  $R16$ , and then concatenating them;

- application of the permutation  $IP^{-1}$ , the inverse of that of the DES start, in order to obtain the 64-bit word  $f'$  forming the encrypted message  $C$ .

The operation SBOX is detailed in Figures 5 and 6. It comprises a constants table  $TC_0$  for supplying an output data item  $a$  as a function of an input data item  $b$ .

In practice, this constants table  $TC_0$  comes in the form of eight elementary constants tables  $TC_{01}$  to  $TC_{08}$ , each receiving at the input only 6 bits of the word  $b$ , for supplying at the output only 4 bits of the word  $a$ .

Thus, the elementary constants table  $TC_{01}$  depicted in Figure 6 receives, as input data, the bits  $b1$  to  $b6$  of the word  $b$  and supplies, as output data, the bits  $a1$  to  $a4$  of the word  $a$ .

In practice these eight elementary constants tables  $TC_{01}$  to  $TC_{08}$  are stored in the program memory of the electronic component.

In the operation SBOX of the first cycle  $T1$ , a particular bit of the output data  $a$  of the constants table  $TC_0$  depends on solely 6 bits of the data  $b$  applied at the input, that is to say on solely 6 bits of the secret key  $K$  and the input message  $(M)$ .

In the operation SBOX of the last cycle  $T16$ , a particular bit of the output data  $a$  of the constants table  $TC_0$  can be recalculated from solely 6 bits of the secret key  $K$  and the encrypted message  $(C)$ .

However, going back to the principle of the DPA attack, if one or more bits of the output data are chosen as target bits, it is sufficient to make a hypothesis on 6 bits of the key  $K$  in order to predict the value of the target bit or bits for a given input message ( $M$ ) or output message ( $C$ ). In other words, for the DES, it is sufficient to make a hypothesis on a 6-bit sub-key.

In a DPA attack on such an algorithm for a given set of target bits issuing from a given elementary constants table, a correct sub-key hypothesis has therefore to be distinguished from among 64 possible ones.

Thus, from the output bits of the eight elementary constants tables  $TC_01$  to  $TC_08$ , up to  $8 \times 6 = 48$  bits of the secret key can be discovered, by carrying out DPA attacks on corresponding target bits.

In the DES, critical instructions in the DPA attack sense are therefore found at the start of the algorithm and at the end. These instructions are detailed in the French patent application FR 98 13605 to which reference can usefully be made.

And it emerges that all the data manipulated by critical instructions are an output data item or data derived from an output data item of a DES start and end SBOX operation.

The countermeasure method described in the aforementioned French patent application applied to this DES algorithm consists in making each of the data items manipulated by the critical instructions

unpredictable. Thus, whatever the target bit or bits used, the signal  $DPA(t)$  will always be null. This countermeasure method is applied to the DES start critical instructions and to the DES end critical instructions.

By taking the SBOX operations as first calculation means for supplying an output data item  $S=a$  from an input data item  $E=b$ , the countermeasure method of the aforementioned French patent application applied to the DES algorithm consists in using other calculation means instead of the first, in order to make the output data item unpredictable, so that this output data item and/or derived data manipulated by the critical instructions are all unpredictable.

These other means can comprise various means. They are calculated from the first means by applying an EXCLUSIVE OR with a random value  $u$  (or a derived random value) to one and/or the other of the input and output data of the first means.

The use of this random value  $u$  is such that the result at the output of the algorithm, that is to say, the encrypted message  $C$ , remains correct.

Figures 7 and 8 depict an example application of this countermeasure method, which corresponds to Figure 10 of the aforementioned French patent application.

In a conventional execution of the DES algorithm, it has been seen that each cycle comprises the use of first means  $TC_0$  in an operation SBOX.

In this example, and as depicted in Figure 7, other means are calculated by performing an EXCLUSIVE



OR with a random value  $u$  on the output data of the first means  $TC_0$  and by performing an EXCLUSIVE OR with a derived value  $e(p(u))$  on the input data of the first means  $TC_0$ . Then an identical execution sequence SEQ $A$  is applied to each group, which consists in using these other calculated means.

In this method, use is therefore made of a random value  $u$  which is a 32-bit data item. For example, a 32-bit random value can be taken, or else a 4-bit random value can be taken and copied 8 times in order to obtain a 32-bit random value.

The derived variable equal to  $e(p(u))$  is then calculated, where  $p(u)$  corresponds to the result of the operation  $P$  PERM applied to the value  $u$  and where  $e(p(u))$  is the result of the operation EXP PERM applied to the value  $p(u)$ .

The other means used by this countermeasure method can then be calculated.

In the example depicted with reference to Figure 7, these other means comprise second means  $TC_2$  and an additional EXCLUSIVE OR operation denoted CP.

The second means  $TC_2$  are used in each of the cycles.

They are calculated by applying an EXCLUSIVE OR with the derived random variable  $e(p(u))$  to the input data  $E$  and applying an EXCLUSIVE OR with the random value  $u$  to the output data  $S$  of the first means  $TC_0$ , which can be written:

$$TC_2 = (E \oplus e(p(u)), S \oplus u).$$

The additional EXCLUSIVE OR operation CP with the derived random variable  $e(p(u))$  makes it possible to obtain, at the input of the second means  $TC_2$ , the data  $b \oplus e(p(u))$ . This operation is denoted  $CP(e(p(u)))$  in Figures 7 and 8.

This additional EXCLUSIVE OR operation CP with the variable  $e(p(u))$  can be placed in various locations in the first and last cycles, either between the operation EXP PERM and the operation XOR or between the operation XOR and the operation SBOX. It can be replaced by an additional EXCLUSIVE OR operation CP with the derived random variable  $p(u)$ , by placing this additional operation  $CP(p(u))$  before the operation EXP PERM.  $l \oplus e(p(u))$  is obtained at the output, and this will therefore then give  $b \oplus e(p(u))$ .

In all these cases, the data  $b \oplus e(p(u))$  is obtained at the input of the operation SBOX.

The calculation program then consists, at the start of execution of the algorithm, in taking a random value  $u$ , in the example a 4-bit value, of calculating the derived random variable  $e(p(u))$ , and then of calculating the various means used in the execution sequence SEQA, that is to say calculating the second means  $TC_2$ .

At the output of each group, the correct result for the output parameters is obtained. Thus, the output parameters  $L4$  and  $R4$  of the first group  $G1$ ,  $L8$  and  $R8$  of the second group  $G2$ ,  $L12$  and  $R12$  of the third

group G3, and L16 and R16 of the fourth group G4 are correct whatever the random variable taken.

When all the cycles have been performed, the correct parameters L16 and R16 are obtained which will make it possible to calculate the correct encrypted message C.

On the other hand, within the groups, certain intermediate results do not have the same values according to the sequence used, but values corresponding to the EXCLUSIVE OR operation with the random value  $u$  or with the derived random value  $e(p(u))$ , which makes it possible to obtain protection against DPA attacks.

Figure 8 shows the detailed flow diagram of the four cycles T1, T2, T3 and T4 of the first group G1, in the sequence SEQA, which makes it possible to reveal the role of the second means  $TC_2$  used in each cycle. According to their definition:  $TC_2 = E \oplus e(p(u))$ ,  $S \oplus u$ ; by applying at the input the randomly modified data  $b \oplus e(p(u))$  by means of the additional operation CP, the randomly modified data  $a \oplus u$  is obtained at the output. Taking this reasoning from the cycle T1 to the end of the cycle T4, and noting that  $p(u) \oplus p(u) = 0$ , the unmodified data L4, R4 are obtained at the output of the cycle T4.

With such a countermeasure method, taking of the random value  $u$  and calculation of the means used in the execution sequence SEQA must be provided at the DES start. These means, calculated at each execution of

the DES, are stored, at execution time, in working memory, the first means  $TC_0$  which are used for the calculation being themselves stored in program memory.

This countermeasure method according to the state of the art, which therefore consists in general terms in applying a random value  $u$  at least to the output of the calculation means used in each cycle of the algorithm, leaves certain data in clear. In Figures 7 and 8 it can be seen that the input data,  $L_0$ ,  $R_0$ , and following them the data  $h$ ,  $l$  and  $b$  of the first cycle, are used in clear.

Similarly, the data  $R_3$ ,  $L_4$ ,  $R_4$ ,  $R_7$ ,  $L_8$ ,  $R_8$ ,  $R_{11}$ ,  $L_{12}$ ,  $R_{12}$ ,  $R_{15}$ ,  $L_{16}$  and  $R_{16}$  are used in clear.

In general terms, whatever the mode of application of the countermeasure method of the state of the art which has just been described, at least the input data  $L_0$  and  $R_0$  and output data  $L_{16}$  and  $R_{16}$  are used in clear in the algorithm. Other intermediate data may be so, as in the case described previously, which depend more particularly on the considered mode of application of the countermeasure method of the state of the art, of which Figures 7 and 8 show only one of the example applications.

In practice, attacks can therefore still be carried out on the algorithm, based on these data used in clear.

The present invention therefore proposes an improvement to the aforementioned countermeasure method, which makes it possible to make all the data used in the algorithm unpredictable, by means of either

the first random value  $u$ , or a second random value denoted  $v$ , or a combination of the two.

An example implementation of this method is depicted in Figure 9.

According to the invention, a second random value denoted  $v$  is used, applied to the input data  $L0$  and  $R0$ , by means of an EXCLUSIVE OR operation.

Thus, the input data actually used in the calculation of the algorithm are unpredictable data equal to  $L0 \oplus v$  and  $R0 \oplus v$ .

This second random value propagates through each of the cycles of the algorithm. At the output of the sixteenth cycle  $T16$ , the unpredictable data equal to  $L16 \oplus v$  and  $R16 \oplus v$  are therefore obtained as output data.

In order to rediscover the true output data  $L16$  and  $R16$  which will make it possible to obtain the encrypted message  $C$ , an EXCLUSIVE OR operation with the second random value  $v$  is applied to each of these data items  $L16 \oplus v$  and  $R16 \oplus v$ .

The use of the two random values  $u$  and  $v$  in combination makes it possible to obtain an improved countermeasure method, making the DES algorithm which implements it impervious to attack.

Figure 9 shows the detail of a practical example implementation of a countermeasure method according to the invention.

If the first cycle  $T1$  is taken, there are at the input the data items  $L0 \oplus v$  and  $R0 \oplus v$  to which the operations EXP PERM and XOR (with the key  $K1$ ) are

applied successively. The data at the input of the next operation SBOX is therefore the data  $b \oplus v$ .

The calculation means  $TC_M$  associated with this operation SBOX consist, as in the countermeasure method of the state of the art, of a constants table deduced from the original constants table  $TC_0$  of the DES algorithm.

Denoting this original constants table  $TC_0 = (E, S)$  as seen in connection with Figure 6, the new calculation means  $TC_M$  are calculated as follows:

$$TC_M = (E \oplus e(v), S \oplus u).$$

In this way, the second random value  $v$  applied to the data at the input of each cycle is taken into account, and benefit is still obtained from the first random value,  $u$ , according to the method of the state of the art, at the output of the operation SBOX.

Thus, at the output of the operation SBOX using the calculation means  $TC_M$ , the data  $a \oplus p(u)$  is obtained, to which the operation P PERM is applied, giving the data  $c \oplus p(u)$ .

The following XOR operation with the input data  $L0 \oplus v$  supplies at the output the data  $g \oplus p(u) \oplus v$ .

It should be noted that, in the state of the art described (Fig. 8), at this stage the data  $g \oplus p(u)$  used at the input of the second cycle T2 was obtained.

With the method according to the invention, the other input of the second cycle is the data  $L1 \oplus v = R0 \oplus v$ , as shown in Figure 9.

The second random value  $v$  therefore propagates through all the cycles of the algorithm.

If the random value  $u$  is not eliminated from the output data of the first cycle ( $R1 \oplus (v) \oplus p(u)$ ), it is necessary to make provision for the use of other calculation means  $TC_M'$  in the second cycle  $T2$ , defined by  $TC_M' = E \oplus e(v) \oplus e(p(u)), S \oplus u$ .

This implementation of the invention is not of great interest, since it necessitates the calculation of two new constants tables  $TC_M$  and  $TC_M'$ , the random value  $u$  being applied in the table  $TC_M'$ , not only to the output, but also to the input.

Also, according to the invention, and as depicted in Figure 9, in order to facilitate the use of the two random variables  $u$  and  $v$  by reducing the calculations necessary for its implementation and in order to repeat the same operations in each cycle, an additional EXCLUSIVE OR operation denoted  $CP(p(u))$  is provided at the end of each cycle, so as to eliminate the value  $p(u)$  at the input of each new cycle. Thus, at the input of the second cycle  $T1$ , the data  $R1 \oplus v = (g \oplus p(u) \oplus v) \oplus p(u)$  is obtained, that is

$$R1 \oplus v = g \oplus v.$$

Each cycle then follows the previous one, executing the same sequence of calculation operations, so that, at the output of the sixteenth cycle,  $L16 \oplus v$  and  $R16 \oplus v$  are obtained as output data. By applying an EXCLUSIVE OR operation with the second random value  $v$  to each of these two data items, the data  $L16$  and  $R16$

are obtained which allow the encrypted message  $C$  to be produced.

By applying the countermeasure method according to the invention which combines the use of a first random value  $u$  in calculation means provided in each cycle and the use of a second random value applied at the input, before the execution of the first cycle, all the data used in the algorithm are made unpredictable. Depending on the location in the algorithm, the countermeasure protection according to the invention is provided either by the first random value  $u$ , or by the second random value  $v$ , or by a combination of these two values.

In practice, and in the example application depicted in Figure 9, before executing the DES algorithm proper, it is necessary to execute the following operations:

- taking of the random values  $u$  and  $v$
- calculation of  $p(u)$  for the operation  $CP(p(u))$
- calculation of  $e(v)$
- calculation of  $TC_M = E \oplus e(v), S \oplus u$ .

The random value  $v$  is a data item having the same number of bits as the data items  $L0$  and  $R0$ , that is 32 bits in the example. In this method, use is therefore made of a random value  $v$  which is a 32-bit data item. For example, a 32-bit random value can be taken, or else a 4-bit random value can be taken and copied 8 times in order to obtain a 32-bit random value (as for the random value  $u$ ).



Other example applications can be envisaged, in which notably it can be provided that the cycles are not identical. All these variants which use the two random values according to the general principle explained are within the scope of the invention.

An electronic component 1 implementing a countermeasure method according to the invention in a DES secret key cryptographic algorithm comprises typically, as depicted in Figure 10, a microprocessor mP, a program memory 2 and a working memory 3. The various calculation means  $TC_0$  and  $TC_M$  are, in practice, constants tables stored respectively in program memory 1 and in working memory 3. In order to be able to manage the use of these calculation means, means 4 of generating a random value are provided which, if reference is made to the flow diagrams of Figures 7 and 11, will supply the random values  $u$  and  $v$  at each execution of the DES. Such a component can most particularly be used in a smart card 5, in order to improve its inviolability.

## CLAIMS

1. A countermeasure method in an electronic component implementing a secret key (K) cryptographic algorithm, the implementation of which comprises a number of successive calculation cycles (T1, ... T16) in order to supply, from first input data (L0, R0) applied to the first cycle (T1), final data (L16, R16) at the output of the last cycle (T16) allowing the production of an encrypted message (C), each calculation cycle using calculation means (TC) for supplying an output data item (S) from an input data item (E), said calculation means comprising the application of a first random value (u) in order to obtain at the output an unpredictable data item ( $S \oplus u$ ), characterised in that the method comprises the use of means of applying a second random value (v) to said first input data (L0, R0), according to an EXCLUSIVE OR operation.

2. A countermeasure method according to Claim 1, characterised in that it also comprises the use of means of applying the second random value (v) to the final data supplied by the last cycle (T16), according to an EXCLUSIVE OR operation.

3. A countermeasure method according to either one of the previous claims, characterised in that it comprises, at the end of each cycle, the execution of an additional operation ( $CP(p(u))$ ) in order to eliminate said first random value (u) at the output of each cycle.

4. A countermeasure method according to any one of the previous claims, characterised in that it comprises the taking of first and second random values ( $u$ ,  $v$ ) and calculation of the calculation means ( $TC_M$ ) used in each cycle for each new execution of the algorithm.

5. A method according to Claim 4, characterised in that said calculation means ( $TC_M$ ) are calculated from first calculation means ( $TC_0$ ) defining, for input data ( $E$ ), corresponding output data ( $S$ ), by applying the second random value ( $v$ ) to said input data ( $E \oplus e(v)$ ) and applying the first random value ( $u$ ) at least to said output data ( $S \oplus u$ ) of the first calculation means.

6. A countermeasure method according to Claim 5, characterised in that the calculation means ( $TC_0$ ,  $TC_M$ ) are constants tables.

7. An electronic security component implementing the countermeasure method according to either one of Claims 5 or 6, characterised in that the first calculation means ( $TC_0$ ) are fixed in program memory (1) of said component, the calculation means ( $TC_M$ ) used in each cycle being calculated at each new execution of the algorithm and stored in working memory (3), and in that it comprises means (4) of generating first and second random values ( $u$ ,  $v$ ) for calculating said calculation means ( $TC_M$ ).

8. A smart card comprising an electronic security component according to Claim 7.